EXHIBIT 1

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF TEXAS

HOUSTON DIVISION

IN RE APACHE CORP. SECURITIES LITIGATION	Case No. 4:21-cv-00575 District Judge George C. Hanks, Jr. Magistrate Judge Andrew M. Edison CLASS ACTION

LEAD PLAINTIFFS' PROPOSED DISOVERY PROTOCOL REGARDING PRODUCTION OF ESI AND PAPER DOCUMENTS

Lead Plaintiffs in the above-captioned case (the "Action"), by and through their counsel, submit this Proposed Discovery Protocol Regarding Electronically Stored Information and Paper Documents (the "Protocol") to govern the searching, identification, processing, and production of hard copy ("Hard Copy Materials") and electronically stored documents and information ("ESI," and together with Hard Copy Materials, "Discovery Material") in the Action.

I. GENERAL PROVISIONS

1. Nothing in this Protocol is intended to alter the Parties' rights under or obligations to comply with any applicable Federal Rules of Civil Procedure, Local Rules of the United States District Court for the Southern District of Texas (the "Local Rules"), or the Court's Court Procedures (the "Procedures") regarding the production of Hard Copy Materials or ESI.

2. No provision of this Protocol waives any objections as to the relevance, discoverability, admissibility, or confidentiality of any particular Discovery Material produced in this Action. For the avoidance of doubt, a Party's compliance with this Protocol will not be

interpreted to require disclosure of information potentially protected by the attorney-client privilege, the work product doctrine, or any other applicable privilege.

3. To the extent that any Party collected and processed documents in response to a discovery request in this Action before the Parties' agreement to this Protocol, and production of such documents was not made in accordance with the terms of this Protocol, the Parties will meet and confer if the other Parties have questions or concerns about the format of any such productions.

4. References to deadlines in this Protocol shall comply with Federal Rule of Civil Procedure 6 with respect to computing deadlines.

5. Production of responsive, non-privileged documents shall be completed on a rolling basis. The Parties agree that Documents may be produced without a prior meet-and-confer.

6. The Parties may mutually modify or revise this Protocol by agreement as circumstances dictate.

7. The Parties shall meet and confer in an effort to resolve any disputes that may arise under this Protocol before seeking relief from the Court.

II. DEFINITIONS

1. "Archival systems" mean long-term repositories for the storage of records that preserve the content of the documents or data stored therein, prevent or track alterations to such documents or data, and control access to electronic records.

2. "Back-up systems" refers to computer systems used to store copies of electronic information on back-up media (magnetic tapes, CDs, DVDs, hard drives, or other storage), to permit recovery of the information in the event of loss or damage to the original data.

3. "Custodial Data Sources" means any potentially relevant data sources unique to any particular individual that are in the possession, custody, or control of a Party, and may include, but are not limited to, any applicable local hard drives, network home or personal file shares,

removable storage, email, online or cloud storage (e.g., OneDrive, SharePoint), removable storage media, messaging applications or software, communication, or coordination platforms (e.g., Microsoft Teams), phones, tablets, laptops, and physical files.

4. "Document" shall have the meaning contemplated by Federal Rule of Civil Procedure 34(a)(1)(A), which includes Electronically Stored Information ("ESI").

5. "Electronic message" means any electronic text or media content exchanged between two or more users of a software application, including but not limited to SMS messages sent over cellular networks and messages sent over the Internet using WhatsApp, iMessage, and Microsoft Teams (instant messaging), among other applications.

6. "Email" means an electronic means for communicating written information that is deliverable to designated recipients at specific addresses associated with particular Internet domains.

7. "Extracted text" means the text extracted from a Native document, and includes all header, footer and document body information when available.

8. "Load file" means an electronic file used to import required production information into a document database, including, document images, extracted text or OCR text, native files, and metadata, as well as information indicating document breaks and relationships (*e.g.*, parent-child relationships for email families).

9. "Metadata" means structured data about ESI that is created by the file system or application, embedded in the document, and as modified through ordinary business use, that describes the characteristics, origins, usage, and validity of the ESI, among other things.

10. "Native format" means the format of ESI in the application in which such ESI was originally created.

11. "Network" or "shared storage systems" shall mean any data storage device accessible to multiple users remotely over a computer network.

12. "Non-Custodial Data Sources" means any potentially relevant enterprise, network or shared data sources accessible by multiple individuals that are in the possession, custody, or control of a Party and may include, but are not limited to, any applicable databases, file servers, storage area networks (SANs), network-attached storage (NASs), email servers or platforms, web servers or platforms, communication or coordination platforms (e.g., Microsoft Teams), third-party-hosted Software as a Service (SaaS) platforms, document management systems (DMS), record management systems (RMS), content management systems (CMS), departmental/project/collaborative/shared storage spaces, e-rooms, structured data stores, application data, online or cloud storage (e.g., OneDrive, SharePoint), back-up systems or media, archival systems, and hard-copy document repositories.

13. "OCR" means the optical character recognition technology used to read hard copy paper documents or electronic images of documents, and output such documents to a searchable text format.

14. "Producing Party" means any Party that produces documents or ESI pursuant to this Protocol.

15. "Receiving Party" means any Party that receives documents or ESI produced in this Action.

16. "Requesting Party" means any Party that requests production of documents or ESI in this Action.

17. "Responsive document" means any document or ESI that a Party produces in response to any discovery request or subpoena served in this Action, subject to any limitations

under the Federal Rules of Civil Procedure, Local Rules, Procedures, or order of this Court.

18. "Search term" means a word or a combination of words or phrases designed to capture potentially relevant ESI and includes strings of words and phrases joined by proximity and Boolean connectors or other syntax.

19. "Structured data" means data that resides in a fixed field within a record or file, or stored in a structured format, such as databases (such as Oracle, SQL, Access) or data sets, according to specific form and content rules as defined by each field of the database.

20. "Tagged Image File Format" or "TIFF" refers to the Group IV graphic file format for storing bit-mapped images of documents and ESI.

21. "TAR" (Technology-Assisted Review) means a process for prioritizing or coding a collection of ESI using a computerized system, using algorithms or systematic rules, that harnesses human judgments of subject matter expert(s) on a smaller set of documents and then extrapolates those judgments to the remaining documents in the collection. TAR systems generally incorporate statistical models and/or sampling techniques to guide the process and to measure overall system effectiveness.

22. "Text file" is a file containing the full text of native files extracted directly from the native file, or, in the case of hard copy documents or scanned PDF documents, subject to OCR, a file containing the text resulting from the OCR.

23. "Unstructured data" refers to free-form data which either does not have a data structure or has a data structure not easily readable by a computer without the use of a specific program designed to interpret the data, including but not limited to, word processing documents, slide presentations, email, PDFs, spreadsheets, and webpages, blogs, image files, instant messages, audio and video files, and others of similar variable format.

III. COLLECTION AND PROCESSING

A. The parties shall use methods of collection and processing (a) that preserve the integrity of document metadata, (b) that preserve parent-child and family group relationships such as the association between parent documents and attachments, (c) that preserve the relationship between emails, electronic messages, chats, or channel messages (e.g., within Microsoft Teams) that contain links to cloud attachments (e.g., within SharePoint or Teams) and the cloud attachments so linked, and (d) that extract embedded files from Documents, subject to paragraph III.C below.

B. **Discovery Not Required**. Except as otherwise agreed to by the Parties or ordered by the Court, the Parties need not collect the following ESI:

a. Data stored on photocopiers, scanners, and fax machines.

b. Any electronic file which matches the Reference Data Set published by the National Institute of Standards and Technology's National Software Reference Library.

c. System or executable files (.exe, .dll, etc.).

d. Structural files not material to individual file contents that do not contain substantive content (.css, .xsl, .xml, .dtd, etc.).

e. Documents from data sources that a party claims are inaccessible due to undue burden or cost.

f. Backup data files that are maintained in the normal course of business for purposes of disaster recovery, including backup tapes, discs, SAN, and other forms of media, and are substantially duplicative of data that is more accessible elsewhere.

g. Deleted, slack, fragmented, or unallocated data.

h. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

i. On-line access data such as temporary internet files, history files, cache files, and cookies.

j. Data in metadata fields frequently updated automatically, such as last-opened or last-printed dates, except to the extent specified in the Metadata Field Table attached hereto.

k. Data remaining from systems no longer in use that are unreadable on the systems in use.

l. Other standard system file extensions, including but not limited to BIN, CAB, CHK, CLASS, COD, COM, DLL, DRV, INF, INI, JAVA, LIB, and SYS.

C. Embedded Objects. Logos, icons, and footers that are embedded in Documents may be culled from a data set and need not be produced as separate documents by a Producing Party (e.g., such embedded objects will be produced within the document itself, rather than as separate attachments).

IV. SEARCH METHODOLOGY

A. Transparency and Cooperation. The Parties agree to be reasonably transparent regarding the universe of documents subject to collection and the methodologies being used to identify responsive documents. If, after reviewing Discovery Materials received from the Producing Party, the Requesting Party believes that additional searches or collections may be necessary, it shall request a meet-and-confer to determine what, if any, additional searches the Producing Party is willing to conduct.

B. Custodians. Each Producing Party will disclose a list of the document custodians whose data will be searched for responsive documents, as well as the Custodial Data Sources being searched for each custodian.

C. Non-Custodial Sources. Each Producing Party will disclose a list of the Non-Custodial Document Sources being searched.

D. Search Terms. Where a Producing Party elects to use search terms to identify documents and ESI potentially responsive to a Party's requests for production, the Producing Party will provide a list of proposed search terms that it believes would lead to the identification of responsive documents and ESI. Within 5 business days of receiving the Producing Party's proposed search terms, the Requesting Party will provide any proposed revisions to the terms. Within 5 business days of receipt of the Requesting Party's proposed revisions, the Producing Party will identify the terms that it is willing to run and any modifications that it is willing to make to its proposed search terms in light of the Requesting Party's proposed revisions. If disputes still exist at the end of that process, the Parties may submit them to the Court pursuant to the Court's practices and procedures for raising discovery disputes.

E. Technology-Assisted Review. Where a Producing Party elects to use predictive coding/technology-assisted review, instead of search terms, to identify documents and ESI potentially responsive to a Party's requests for production, the Producing Party will disclose (i) the data sources against which TAR will be run; (ii) the TAR or advanced analytics methodology deployed; (iii) the quality control measures used to validate the results, including recall and precision rates; (iv) any documents, document types, file types, or other categories of ESI to be excluded from the TAR process; and (v) the method used to identify such documents for exclusion. If any Party has concerns about another Party's TAR protocol, the Parties will meet and confer to

try to address them. If disputes still exist at the end of the meet and confer process, the Parties may submit them to the Court pursuant to the Court's practices and procedures for raising discovery disputes. The parties agree that a producing party may not to utilize TAR after application of search terms except to prioritize the review of all documents hitting on the agreed-upon search terms.

F. Validation. The Parties will meet and confer regarding appropriate measures for validating the results of the methodologies applied to identify potentially responsive ESI.

V. PRODUCTION OF HARD COPY DOCUMENTS

Hard copy documents should be scanned as single-page, Group IV, 300 DPI TIFF images and produced with an .opt image cross-reference file and a delimited database load file (*i.e.*, .dat). The database load file should contain the following fields: "BEGBATES," "ENDBATES," "PAGES," "VOLUME," and "CUSTODIAN." The documents should be logically unitized (*i.e.*, distinct documents shall not be merged into a single record, and single documents shall not be split into multiple records) and be produced in the order in which they are kept in the usual course of business. If an original document contains color, the document shall be produced as single-page, 300 DPI JPG images with JPG compression and a high-quality setting as to not degrade the original image. Multi-page OCR text for each document should also be provided. The OCR software shall maximize text quality. Settings such as "auto-skewing" and "auto-rotation" should be turned on during the OCR process. Each text file shall be named with the beginning Bates number of the hard copy document to which the text file relates. The parties agree that should the volume of the Hard Copy Materials make the production of single page 300 dpi JPG images with JPG compression unreasonably burdensome, the parties will meet and confer in efforts to reduce the volume of documents to be produced as single page 300 dpi JPG images with JPG compression (as opposed to black and white TIFF images).

VI. PRODUCTION OF ESI

A. Format. All documents and ESI produced in this Action shall be produced in the formats described below:

a. **Images**. Except as otherwise specified herein, all other documents and ESI shall be produced as single-page, black and white, TIFF Group IV, 300 DPI TIFF images. If an original document contains color and is an image-based file (e.g., .jpeg), or a PowerPoint, or color is material to the understanding of the document, then the document should be produced as single-page, 300 DPI JPG images with JPG compression and a high-quality setting as to not degrade the original image. TIFFs/JPGs shall be processed to show any and all text and images that would be visible to the reader using the native software that created the document (*e.g.*, TIFFs of emails should include the BCC line). To the extent that Excel files and other spreadsheets and other files that are not able to be imaged must be imaged to redact privileged information under the terms herein, they shall be processed in a manner that maintains and displays all hidden columns or rows, hidden text or worksheets, speaker notes, track changes, and comments. However, the Parties are under no obligation to enhance an image beyond how it was kept in the usual course of business. If the image does not accurately reflect the document as it was kept in the usual course of business, the Parties agree to meet and confer in good faith on production format options. Page orientation for TIFF/JPG images shall be the same as the underlying document from which the image is created.

b. **Native Files**. Microsoft Excel and other spreadsheet file types, including comma or tab delimited text files, PowerPoint, and other presentation file types, Microsoft Access files, and audio and video files, photo or graphic images, documents with tracked changes in the metadata, and other file types that – when produced in a non-native format

– limit or lose relevant content, shall be produced in native format. For each document or ESI required to be produced in native format, the Producing Party shall also provide a single-page Bates stamped image slip sheet stating the document has been "PRODUCED IN NATIVE FORMAT." Each native file should be named according to the Bates number it has been assigned and should be linked directly to its corresponding record in the load file using the NATIVELINK metadata field. PowerPoint documents shall be produced in native format along with single-page, 300 DPI TIFF/JPG color-for-color images, as applicable. In the event that any document or ESI produced in image format is: (i) unreadable or illegible; (ii) cuts off or is missing data or information; or (iii) cannot be utilized at a deposition, a Receiving Party may request that such file be produced in native format in accordance with the procedures outlined in this paragraph, and the Producing Party will comply with all such reasonable requests. To the extent a Receiving Party believes that any other documents or ESI should be produced in native format, it will identify such documents or ESI and the basis for the request, and the Producing Party will either produce the native files or explain why it refuses to produce the native files, and the Parties agree to meet and confer regarding such requests.

c. **Electronic messages**. Electronic messages (e.g., iMessage, SMS, MMS, Teams Chat) shall be produced in a searchable format that preserves the presentational features of the original message, such as emojis, images, video files, animations, and the like to the extent reasonably possible, and shall be produced with its relevant conversation thread broken down by conversation day, along with relevant contextual messages a Producing Party reasonably identifies. To the extent a Requesting Party reasonably believes additional contextual messages are necessary to understand a particular responsive

message, the Requesting Party shall identify the responsive message by Bates number, and Parties will meet and confer regarding what, if any, relevant, non-privileged contextual messages exist for possible production. To the extent a Requesting Party believes that an electronic message was not produced in a searchable format that preserved the presentation features of the original message, the Requesting Party shall identify the message by Bates number, and the Producing Party will reproduce it in a searchable format that preserves the presentation features of the original message if possible.

d. **Structured Data**. To the extent a response to discovery requires production of discoverable ESI stored in a structured database, the Parties shall meet and confer in an attempt to agree upon a set of queries to be made for discoverable information and generate a report in a reasonably usable and exportable electronic file for review by the Requesting Party. Upon review of the report, the Requesting Party may make reasonable requests for additional information, including different reports or report formats, and specific data from identified fields.

e. **Proprietary Software.** To the extent that relevant ESI cannot be rendered or reviewed in a reasonably useable form without the use of proprietary software, the Parties will meet and confer to determine whether and to what extent producing such ESI is necessary and, if so, how that can be accomplished.

f. **Attachments**. If any part of an email or its attachments is responsive, the entire email and all attachments shall be produced, except: (i) where an attachment is withheld pursuant to a valid claim of privilege, in which case that attachment will be replaced with a single-page TIFF image identifying the privilege or work product protection being claimed, and the rest of the family produced; and (ii) where the attachment

is a non-substantive, automatically generated embedded file (*e.g.*, logos) or formatting file (*e.g.*, .ole or .dll). Attachments shall be produced sequentially after the parent email. For such attachments, the BEGATTACH and ENDATTACH metadata fields shall be populated to show the family relationship.

g. **Modern or Cloud Attachments/Hyperlinked Documents**. Documents sent via links to internal or non-public documents (e.g., to Microsoft 365, SharePoint, etc.) that are contained within an email, message, chat or other document, shall be extracted and produced as an attachment, with the parent-child relationship preserved and Metadata fields showing the family relationship and FilePath to such documents populated.

h. **Embedded Files**. Except as set forth above in § III.C, embedded documents or files embedded in documents (e.g., embedded MS Office files) and images embedded in RTF files shall be extracted as separate files and treated as attachments in accordance with the procedures described herein in the prior subsection (§ VI.A.f) with the parent/child relationship preserved.

i. **Dynamic Fields.** All dynamic date and time fields, where such fields are processed to contain a value, shall, to the extent reasonably possible, be processed with a single date and time setting that is consistent across each Party's productions, Coordinated Universal Time (UTC), and in a way that maintains the date/time shown in a document as it was last saved by the custodian or end user, not the date of collection or processing (i.e., force off auto data).

j. **Hidden Content, Speaker Notes, Comments, and Tracked Changes**. To the extent that a document contains hidden content, tracked changes, comments, notes, or other similar information, it shall be imaged so that such information is captured on the

produced image file as it would appear in the native format of the document subject to any claim of privilege or work product protection, in which case redactions will be applied.

k. **Compressed File Types**. Compressed file types (*e.g.*, .ZIP, .RAR, .CAB, .GZ) should be decompressed so that the lowest level document or file is extracted.

l. **Encrypted Files**. Certain files may contain encrypted data or be password protected. Encrypted data and password protected files will be produced only where the key or password can be ascertained after reasonable efforts. To the extent an encrypted or password protected file is inaccessible to the Producing Party but deemed potentially responsive, to the extent available and not subject to a claim of privilege, the Party will identify the file attributes (directory, size, name, extension, last modification date) of any such inaccessible encrypted or password protected files.

B. De-Duplication. Prior to production, each Party will remove exact duplicate stand-alone documents and document families, as identified based on ESI using hash value matching (such as MD5 or SHA-1 hash values). Documents and document families that are not duplicates may not be removed. No Party shall identify and/or eliminate electronic duplicates by manual review or some method other than by use of the technical comparison using MD5 or SHA-1 hash values outlined above. The Parties will de-duplicate globally across the document collection. Duplicate documents held in different file path locations and/or by different custodians do not need to be produced, provided that the load file produced must include a Custodian-All metadata field that shows each custodian from whom or which a copy of the produced document was collected. The Parties shall de-duplicate stand-alone documents against stand-alone documents and shall de-duplicate entire document families against entire document families, in a manner that does not break apart families and shall be performed at a family level.

C. Email Threading. Where an email chain consists of more than one segment, the Producing Party may use industry-standard email threading technology such that only the most inclusive message(s) (i.e., those containing a full and complete reflection of all the text and attachments contained anywhere within the email chain), any lower-included emails that have attachments, and any lower-included email that contains unique content not included elsewhere in a produced email string must be produced. To the extent a Producing Party applies email threading, it shall produce metadata (including email header information) for all lesser included emails that are not independently produced. To the extent a Receiving Party reasonably believes that a lesser-inclusive email should be produced, it may identify those documents by Bates number, and the Parties agree to meet and confer regarding production.

D. Redactions. A Party may only apply redactions to protect attorney-client privilege; attorney work product; joint defense privilege; highly confidential business information (as described below); information prohibited from disclosure by federal, state, or foreign statutes or regulations; personal health information concerning any individual and personal identity information that a Party is required not to disclose by federal, state or foreign statute, or regulation. Redactions shall be limited to the specific privileged information protected and shall not include email header information (unless itself privileged), or factual or contextual information contained in the document. To address particularized concerns regarding the production of sensitive business information contained in the Company's Board materials, the parties agree that a Party also may redact specific highly confidential business information relating to non-relevant businesses contained in Board materials only if (1) the redacted information is both nonresponsive and irrelevant; and (2) the redacted information would not assist in understanding or providing context for the relevant portion of the document or document family of which it is a part. Such redactions

must be identified as "Redacted – Highly Confidential Nonresponsive Information." To the extent a Party is required to withhold from production a member (email or attachment) of an email family on the basis of privilege including work production protection, where some or all of the other email family members are being produced, the producing Party shall provide a Bates numbered placeholder TIFF image bearing the legend, "DOCUMENT WITHHELD FOR PRIVILEGE." To the extent a Party is required to Redact a document required to be produced in Native format under this agreement, it shall to the extent reasonable redact the document using a native redaction tool and, where native redaction is not reasonable, produce the document in a manner that displays all non-privileged information that would be available in the document's native format, including hidden rows and columns for excels and other spreadsheets, speaker notes and comments for Power Points and other presentations, and track changes and comments for Word documents, as well as the date, time and author of any such changes and comments. Redactions will be clearly indicated. For redacted documents, a text file shall be created using OCR and shall be produced in lieu of extracted text. The searchable text file will include the word "Redacted."

E. Bates numbering. Each TIFF/JPG image produced shall be branded with a Bates number that (i) identifies the Producing Party; (ii) maintains a constant length of nine numeric digits (including 0-padding) across the entire production; and (iii) is sequential, both within a given document, but should not include the Bates number in the extracted text of the ESI. Each TIFF/JPG image file shall be named with the same page-level Bates number branded on the underlying image. For ESI that is produced subject to a claim of confidentiality pursuant to the Protective Order entered in this Action (the "Protective Order"), the Producing Party shall electronically brand the appropriate confidentiality designation onto each page of the document, but should not include the confidentiality designation in the extracted text of the ESI.

F. Text Files and OCR. All documents and ESI shall be produced with a corresponding multipage searchable text file (i.e., one .TXT file per electronic file as opposed to one text file per page). The text file for ESI shall contain full text extraction and be created by extracting text directly from the underlying native file, unless the ESI must be redacted prior to production, in which case the text file shall be generated by applying industry standard OCR technology to the redacted version of the ESI. Each text file shall be named with the beginning Bates number of the electronic file to which the text file relates.

G. Load files. All documents should be provided with Concordance-compatible image and data load files (i.e., .OPT and .DAT files) using standard Concordance delimiters showing the Bates number of each page and the approximate unitization of the documents.

H. Metadata. All ESI will be produced with a delimited, database load file that contains the metadata fields listed in Table 1, attached hereto. The metadata produced should have the correct encoding to enable preservation of the documents' original language. For ESI other than email and e-docs that do not conform to the metadata listed in Table 1, such as electronic messages, and ESI from collaboration tools, etc., the Parties will meet and confer as to the appropriate metadata fields to be produced.

I. Production Media. All documents and ESI shall be produced via secure FTP or other secure file transfer or other mutually agreeable production media, along with an identification of the Bates range of the production. Any replacement productions shall be clearly identified as such. All productions shall be encrypted, and the Producing Party shall provide a decryption key at the time of production, via separate cover.

J. Privilege Log. The Parties agree to exchange privilege logs that comply with Federal Rule of Civil Procedure 26(b)(5) on a rolling basis, with the final privilege log being

produced no later than thirty (30) days after the Producing Party has substantially completed its document production. Privilege logs will be provided in a searchable and sortable spreadsheet format. The following privileged communications or work product need not be included in a privilege log unless otherwise agreed to by the Parties or ordered by the Court: (a) communications to or from outside legal counsel related to this Action; (b) work product of counsel and Parties related to this Action; (c) any privileged communications that post-date the filing of the initial complaint in this Action; and (d) any communications regarding litigation holds or preservation, collection, or review of discoverable information in this Action. With respect to e-mail threads for which a Party claims a privilege over one or more of the discrete communications within the thread, only the most inclusive e-mail need be logged, but the log will set forth the basis for the privilege claim for each lesser inclusive email within the thread for which a privilege claim is made regardless of the segment in which the privileged information exists within the inclusive e-email, and shall provide metadata for each of the lesser inclusive emails for which a claim of privilege is made. The Parties will meet and confer in good faith regarding the scope of the privilege log should any such issues arise. Further, the Parties agree that documents that have been redacted for privilege should also be logged separately and include the fields as set forth in the following paragraph.

In an effort to avoid unnecessary expense and burden, the Parties agree that, for documents withheld from production or redacted on the basis of attorney-client privilege, work product doctrine, and/or any other applicable privilege, the Producing Party will prepare a log containing, for each document (except those exempted above): (a) the privilege(s) claimed; (b) the date of the document; (c) the author(s), addressee(s), and all recipients of the document and, to the extent available in the metadata for the logged document, the email addresses for all such persons; (d) a

description of the general subject matter of the privileged information contained in the document sufficient to allow the Receiving Party (and the Court as necessary) to assess the privilege claimed; and (e) the custodian. The log will be accompanied by a list identifying any person on the log who is an attorney or an employee of any legal department. For redacted documents, if there is more than one redaction per document, one log entry can be used to describe the multiple redactions.

If the Receiving Party reasonably requires further information, it shall explain in writing the need for such information and identify, by Bates number or other unique identifier, each document for which it seeks this information. The Producing Party will respond to any such reasonable request by providing a more detailed description of the nature of the withheld information that will enable the Receiving Party to assess the claim of privilege.

If the Receiving Party contests a privilege claim, the Receiving Party must notify the Producing Party in writing. The Parties must attempt to confer in good faith to resolve any challenge. Thereafter, the Parties may seek judicial intervention if the challenge cannot be resolved.

K. Privilege Claw Back. The inadvertent production of privileged or work-product protected data (including metadata) is governed by the applicable Federal Rules of Civil Procedure and the Protective Order entered in the Action.

Dated: April 4, 2023

s/ Joshua E. D'Ancona

KESSLER TOPAZ
MELTZER & CHECK, LLP
Gregory M. Castaldo (admitted *pro hac vice*)
Johnston de F. Whitman, Jr. (admitted *pro hac vice*)
Joshua E. D'Ancona (admitted *pro hac vice*)
Michelle M. Newcomer (admitted *pro hac vice*)
Richard A. Russo Jr. (admitted *pro hac vice*)
Daniel B. Rotko (admitted *pro hac vice*)
Austin W. Manning (admitted *pro hac vice*)
280 King of Prussia Road

Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056
gcastaldo@ktmc.com
jwhitman@ktmc.com
jdancona@ktmc.com
mnewcomer@ktmc.com
rrusso@ktmc.com
drotko@ktmc.com
amanning@ktmc.com

SAXENA WHITE P.A.
David R. Kaplan (admitted *pro hac vice*)
Wolfram T. Worms (admitted *pro hac vice*)
Hani Farah (admitted *pro hac vice*)
505 Lomas Santa Fe Dr., Suite 180
Solana Beach, CA 92075
Telephone: (858) 997-0860
Facsimile: (858) 369-0096
dkaplan@saxenawhite.com
wworms@saxenawhite.com
hfarah@saxenawhite.com

-and-

Steven B. Singer (*pro hac vice* forthcoming)
Joshua H. Saltzman (admitted *pro hac vice*)
Sara DiLeo (admitted *pro hac vice*)
10 Bank Street, 8th Floor
White Plains, NY 10606
Telephone: (914) 437-8551
Facsimile: (888) 631-3611
ssinger@saxenawhite.com
jsaltzman@saxenawhite.com
sdileo@saxenawhite.com

-and-

Maya Saxena (*pro hac vice* forthcoming)
Joseph E. White, III (*pro hac vice* forthcoming)
Lester R. Hooker (*pro hac vice* forthcoming)
7777 Glades Road, Suite 300
Boca Raton, FL 33434
Telephone: (561) 394-3399
Facsimile: (561) 394-3382
msaxena@saxenawhite.com

jwhite@saxenawhite.com
lhooker@saxenawhite.com

Co- Lead Counsel for Lead Plaintiffs

AJAMIE LLP
Thomas R. Ajamie, Attorney-in-Charge
Texas Bar No. 00952400
S.D. Tex. No. 6165
John S. "Jack" Edwards, Jr.
Texas Bar No. 24040851
S.D. Tex. No. 38095
Pennzoil Place – South Tower
711 Louisiana, Suite 2150
Houston, TX 77002
Telephone: (713) 860-1600
Facsimile: (713) 860-1699
tajamie@ajamie.com
jedwards@ajamie.com

Liaison Counsel for Lead Plaintiffs

TABLE 1
Metadata Fields[1]

Field Name	Example/Format	Description
BEGBATES	ABC0000001 (Unique ID)	The Document ID number associated with the first page of a document.
ENDBATES	ABC0000003 (Unique ID)	The Document ID number associated with the last page of a document.
BEGATTACH	ABC0000001 (Unique ID Parent-Child Relationships)	The Document ID number associated with the first page of the parent document.
ENDATTACH	ABC0000008 (Unique ID Parent-Child Relationships)	The Document ID number associated with the last page of the last attachment.
VOLUME	VOL001	The name of CD, DVD, or Hard Drive.
RECORDTYPE	Options: eMail, Attachment, Scanned Doc, eFile	The record type of a document.
SENTDATE	MM/DD/YYYY	The date the email or calendar entry was sent.
SENTTIME	HH:MM	The time the email or calendar entry was sent.
RECEIVEDDATE	MM/DD/YYYY	The date the document was received.
RECEIVEDTIME	HH:MM	The time the document was received.
CREATEDATE	MM/DD/YYYY	The date the document was created.
CREATETIME	HH:MM	The time the document was created.
LASTMODDATE	MM/DD/YYYY	The date the document was last modified.
LASTMODTIME	HH:MM	The time the document was last modified.
MEETING START DATE	MM/DD/YYYY	Start date of calendar entry.
MEETING START TIME	HH:MM	Start time of calendar entry.
MEETING END DATE	MM/DD/YYYY	End date of calendar entry.
MEETING END TIME	HH:MM	End time of calendar entry.
FILEPATH	i.e /JsmithPC/Users/Jsmith/Desktop	The file path from the location in which the document was stored in the usual course of business. This field should be populated for both email and e-files.
AUTHOR	jsmith	The author of a document from extracted metadata.
LASTEDITEDBY	jsmith	The name of the last person to edit the document from extracted metadata.
FROM	Joe Smith <jsmith@email.com>	The display name and email address of the author of an email/calendar item. An email address should always be provided.
TO	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and email address of the recipient(s) of an email/calendar item. An email address should always be provided for every email if a recipient existed.
CC	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and email of the copyee(s) of an email/calendar item. An

Field Name	Example/Format	Description
		email address should always be provided for every email if a copyee existed.
BCC	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and email of the blind copyee(s) of an email or calendar item. An email address should always be provided for every email if a blind copyee existed.
SUBJECT		The subject line of the email/calendar item.
MESSAGE TYPE	Appointment, Contact, Task, Distribution List, Message, etc.	An indication of the email system message type.
IMPORTANCE	Normal, Low, High	Email Importance Flag
TITLE		The extracted document title of a document.
CUSTODIAN		The custodian of a document from which the document originated.
CUSTODIAN-ALL	Smith, Joe; Doe, Jane	All of the custodians of a document from which the document originated, separated by semicolons.
ATTACH COUNT	Numeric	The number of attachments to a document.
FILEEXT	XLS	The file extension of a document.
FILENAME	Document Name.xls	The file name of a document.
FILESIZE	Numeric	The file size of a document (including embedded attachments).
IS EMBEDDED	Yes or No	The yes/no indicator of whether a file is embedded in another document.
HASH		The MD5 or SHA-1 Hash value or "de-duplication key" assigned to a document. The same hash method (MD5 or SHA-1) should be used throughout production.
REDACTED	Yes or No	The yes/no indicator of whether a file contains redactions.
CONVERSATION INDEX		ID used to tie together email threads.
TIMEZONEPROCESSED	PST, CST, EST, etc	The time zone the document was processed in. **NOTE:** This should be the time zone where the documents were located at time of collection.
NATIVELINK	D:\NATIVES\ABC000001.xls	The full path to a native copy of a document.
FULLTEXT	D:\TEXT\ABC000001.txt	The path to the full extracted text of the document. There should be a folder on the deliverable containing a separate text file per document These text files

[1]For any ESI that does not conform to the metadata listed here, the parties will meet and confer as to the appropriate metadata fields to be produced.